Life Cycle Assessment of Vulnerability and Penetration Testing on Systems and Proactive Action Taken to Resolve Possible Attacks on Networks

Veenababu Kannika Sherly

Research Analyst, SMRVD Security Solutions, India.

Abstract

After getting the vulnerability list of the victim, the attacker make a plan for the possible attack. With that list attacker exploit the victim's network or system and compromise his system security and information. But if Victim removes all the vulnerabilities from his system, the attacker would not be able to exploit the victim's network. By applying VAPT technique user can find out the vulnerabilities those can result in various severe attacks like DDoS attack, etc. After finding out the vulnerabilities user can apply countermeasures against them. To make the system vulnerability free, Administrator should find out vulnerabilities in his own network. The administrator should apply complete vulnerability and penetration testing cycle on the system/network. When the administrator would get the list of available vulnerability in his system, he should remove those vulnerabilities. To remove the vulnerabilities, the administrator should apply the necessary patches, updates, install necessary software and other requisite. In this way administrator would remove all vulnerabilities from the network. In this paper we proved vulnerability assessment and penetration testing as a cyber attack prevention technology, how we can provide active cyber attack prevention using vulnerability assessment and penetration testing. We described complete life cycle of vulnerability assessment and penetration testing on systems or networks and proactive action taken to resolve that vulnerability and stop possible attack.

Keywords: VAPT Tools; System Security; Cyber Attack.

1. Introduction

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privilege. Vulnerability are the potential risk for the system. Attacker uses these vulnerability to exploit the system and get unauthorized access and information. Vulnerabilities are big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system security. Hackers were busy launching and trying their hands on different variants of cyber-attacks such as phishing, malware, distributed-denial-of-service (DDoS), denial-of-service (DoS), advanced persistent threat (APT), malicious social media messaging (MSMM), business email compromise (BEC), botnet, ransomware amongst many others [1-12]. In the case of the phishing attack, hackers used harmful links hidden in carefully designed emails to target company employees. Unfortunately, when employees click on such links, they ignorantly download keylogging software onto their computers or devices, giving hostile actors access to their credentials. Hackers can then gain unrestricted access to critical business assets and data of the victim's organization by impersonating a genuine employee.

Though it is almost impossible to have 100% vulnerability free system, but by removing as many vulnerabilities as possible, we can increase system security. The need of Vulnerability Assessment and Penetration Testing is usually underestimated till now. It is just consider as a formality activity and use by very less people [13-27]. By using regular and efficient Vulnerability Assessment, we can reduce substantial amount of risk to be attacked and have more secured systems. In this paper we describe Vulnerability Assessment and Penetration Testing as an important Cyber Attack Prevention Technology. By using VAPT as a Cyber Attack Prevention Technology we can remove vulnerabilities from our system and reduce possibility of cyber-attack. We explained various techniques of Vulnerability Assessment and Penetration Testing. We described complete life cycle of VAPT for proactive defence. This will also provide complete process how to use VAPT as a Cyber Attack Prevention technology.

Much research have been done by researcher in past in Vulnerability Assessment. Computer vulnerability information shows important regularities and those can also be detected and possibly visualized [28-39]. The interdependency of multiple vulnerabilities and exploits in a single network and their effects. Web vulnerability scanner tool 'SecuBat' developed by them. This analyses vulnerability interdependencies and possible attack path into a computer network.

Vulnerability Assessment and Penetration Testing is a step by step process. Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that. These loopholes can provide backdoor to attacker to attack the victim. A system may have access control vulnerability, Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc.

Penetration testing is the next step after vulnerability assessment. Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system. In penetration testing, the tester have authority to do penetration testing and he intently exploit the system and find out possible exploits [40-51]. Vulnerability Assessment and Penetration Testing is a total 9 step process. First of all tester have to decide the scope of the assignment (Black/grey/white box). After deciding the scope, the tester gets information about the operating system, network, and IP address in reconnaissance step. After this tester use various vulnerability assessment technique (explained further) on the testing object to find out vulnerabilities. Then tester analyses the founded vulnerability and make plan for penetration testing. Tester uses this plan to penetrate the victim's system. After penetrating the system, tester increases the privilege in the system [52-54].

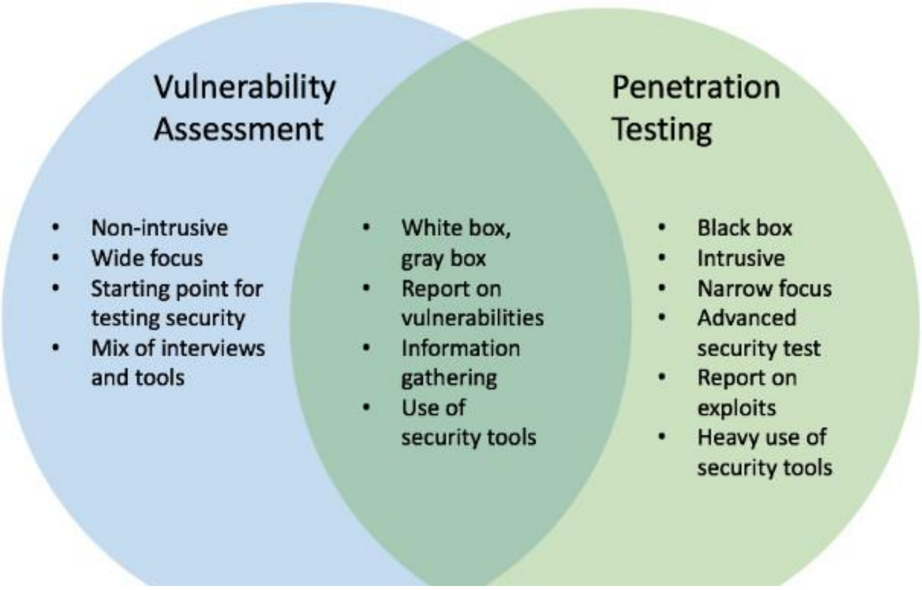

Figure 1. Vulnerability Assessment & penetration testing (Source: Internet)

In result analysis step, tester analyses the all results and devise recommendation to resolve the vulnerability from the system. All these activities are documented and sent to management to take suitable action. After these all step, the victim's system and its program get affected and altered. In cleanup step we restore the system in previous state as it was before VAPT process was started.

2. Vulnerability Assessment Methods

Static analysis - In this technique we do not execute any test case or exploit. We analyze the code structure and contents of the system. With this technique we can find out about all type of vulnerabilities. In this technique we do not exploit system, so there would be no bad effect of this testing on the system. One of the big disadvantage of this technique is that it is quite slow and require many men-hours to perform.

Manual Testing - In this technique, we do not require any tool or any software to find out vulnerabilities. In this tester use his own knowledge and experience to find out the vulnerabilities in the system. This testing can be perform with prepared test plan (Systematic manual testing) or without any test plan (Exploratory manual testing). This technique costs cheaper compare to other techniques, because we do not need to buy any vulnerability assessment tool for this technique.

Automated Testing - In automated testing technique we use automated vulnerability testing tools to find out vulnerabilities in the system. These tools execute all the test cases to find out vulnerabilities. This reduce the men-hours and time required to perform testing. Because of tool repeated testing can also be perform very easily. Automated testing provide better accuracy than what other techniques provide. It takes very less time and same test cases can be used for future operations. But tools increase cost of testing. A single tools is not capable to find out all type of vulnerabilities. So this increase the total cost to perform vulnerability assessment.

Fuzz testing - This is also known as fuzzing. In this we inputs invalid or any Random Data into system and then look for crashes and failure. This is like robustness testing. This technique can be applied with very less human interaction. This technique can be used to find out zero day vulnerability.

Black box testing - In this technique, the tester do not have any prior knowledge of the network architecture or systems of the testing network. Usually black box testing is perform from external network to internal network. Tester have to use his expertise and skills to perform this testing.

Grey box testing - In this technique, the tester have some partial knowledge of the testing network. Tester do not have knowledge of complete network architecture, but he know some basic information of testing network and system configuration. Actually Grey box testing is the combination of both the other techniques. This can be perform from internal or external network.

White box testing - Tester have complete knowledge of the network configuration of the testing network and the system configuration of the testing network/system. Usually this testing is perform from the internal network. White box testing require deep understanding of the testing network or system and gives better results.

Here, we will show how we can consider vulnerability analysis as a Cyber Attack Prevention technology. What usually attacker do is he reconnaissance the victim’s network and get information about victim’s network. After getting information, attacker perform vulnerability assessment on the victim’s network/system and get vulnerability list.

3. Conclusions

Now if the attacker would do vulnerability assessment of the victim’s system/network, he would not find any open vulnerability in the victim’s system/network. In absence of open vulnerabilities in the system, the attacker would not able to exploit victim’s system/network. So by using Vulnerability Assessment and Penetration Testing as a cyber- defence technology administrator can be able to save his resources and critical information and can achieve proactive Cyber Attack Prevention. In this paper we explained how Vulnerability Assessment and Penetration Testing can be used as an effective Cyber Attack Prevention technology. We described why VAPT should be made a compulsory activity for Cyber Attack Prevention . We explained complete life cycle of VAPT, prevalent VAPT techniques and top 15 vulnerability assessment tools.

References

[1] Xiong, P., Peyton, L.: A model driven penetration test framework for web applications. In: IEEE 8th Annual International Conference on Privacy, Security and Trust (2010).

[2] Shah, S., Mehtre, B.M.: A modern approach to cyber security analysis using vulnerability assessment and penetration testing. In: NCRTCST’ 2013, Hyderabad, India.

[3] Shah, S., Mehtre, B.M.: School of Computer and Information Sciences, University of Hyderabad, Hyderabad, India. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

[4] Austin, A., Williams, L.: One technique is not enough: a comparison of vulnerability discovery techniques. In: IEEE International Symposium on Empirical Software Engineering and Measurement (2011).

[5] Vinod Varma Vegesna (2022). "Methodologies for Enhancing Data Integrity and Security in Distributed Cloud Computing with Techniques to Implement Security Solutions," Asian Journal of Applied Science and Technology, Volume 6, Issue 2, Pages 167-180, April-June 2022, doi: 10.38177/ajast.2022.6217.

[6] Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, Hamzah F. Zmezm, Dr. Hussain Falih Mahdi, Hassan Muhsen Abdulkareem Al-Haidari. "Suggested Mechanisms for Understanding the Ideas in Authentication System," International Journal of Advancements in Computing Technology9(3):10-24, 2018.

[7] Hamid Ali Abed Al-Asadi and et al., "Priority Incorporated Zone Based Distributed Clustering Algorithm For Heterogeneous Wireless Sensor Network", Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 5, PP. 306-313, 2019.

[8] Hamid Ali Abed Al-Asadi and et al., "A Network Analysis for Finding the Shortest Path in Hospital Information System with GIS and GPS, Journal of Network Computing and Applications (2020) 5: 10-22.

[9] Vinod Varma Vegesna (2022). "Utilising VAPT Technologies (Vulnerability Assessment & Penetration Testing) as a Method for Actively Preventing Cyberattacks," International Journal of Management, Technology and Engineering, Volume XII, Issue VII, July 2022, Pages 81-94.

[10] Vinod Varma Vegesna (2022). "Accelerate the development of a business without losing privacy with the help of API Security Best Practises - Enabling businesses to create more dynamic applications," International Journal of Management, Technology and Engineering, Volume XII, Issue IX, September 2022, Pages 91-99.

[11] The MITRE Corporation, Common Weakness Enumeration. http://www.cwe.mitre.org/.

[12] SANS Institute. SANS Top 25 Software Errors. http://www.sans.org/top25-software-errors/.

[13] Institute for Security and Open Methodologies. Open Source Security Testing Methodology Manual. http://www.isecom.org/mirror/OSSTMM.3.pdf.

[14] Vinod Varma Vegesna (2018). “Analysis of Artificial Intelligence Techniques for Network Intrusion Detection and Intrusion Prevention for Enhanced User Privacy”, Asian Journal of Applied Science and Technology, Volume 2, Issue 4, Pages 315-330, Oct-Dec 2018, Available at SSRN: https://ssrn.com/abstract=4418114

[15] Hamid Ali Abed Al-Asadi, Majida Ali Abed, AL-Asadi, Zainab sabah, Baha Al-Deen, Ahmad Naser Ismail, “Fuzzy Logic approach to Recognition of Isolated Arabic Characters”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1, 1793-8201, February, 2010.

[16] H. A. Al-Asadi, M.H. Al-Mansoori, S. Hitam, M. I. Saripan, and M. A. Mahdi, “Particle swarm optimization on threshold exponential gain of stimulated Brillouin scattering in single mode fibers,” Optics Express, vol. 19, no. 3, pp. 1842-1853, 2011.

[17] Majida Al-Asadi, Yousif A. Al-Asadi, Hamid Ali Abed Al-Asadi, "Architectural Analysis of Multi-Agents Educational Model in Web-Learning Environments," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 6, 2012.

[18] Vinod Varma Vegesna (2017). “Incorporating Wireless Sensor Networks and the Internet of Things: A Hierarchical and Security-Based Analysis,” International Journal of Current Engineering and Scientific Research, Volume-4, Issue-5, Pages 94-106, Available at SSRN: https://ssrn.com/abstract=4418110

[19] Vinod Varma Vegesna (2016). “Threat and Risk Assessment Techniques and Mitigation Approaches for Enhancing Security in Automotive Domain,” International Journal of Management, Technology And Engineering, Volume VI, Issue II, July-Dec 2016, Pages 314-331, Available at SSRN: https://ssrn.com/abstract=4418100

[20] Vinod Varma Vegesna (2015). “Incorporating Data Mining Approaches and Knowledge Discovery Process to Cloud Computing for Maximizing Security,” International Journal of Current Engineering and Scientific Research, Volume-2, Issue-6, Pages 118-133, Available at SSRN: https://ssrn.com/abstract=4418107

[21] Payment Card Industry Security Standards. Payment Card Industry Data Security Standard. http://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

[22] Shah, S.: Vulnerability assessment and penetration testing (VAPT) techniques for cyber defence. IET-NCACNS' SGGS, Nanded (2013).

[23] Vinod Varma Vegesna (2022). "Investigations on Cybersecurity Challenges and Mitigation Strategies in Intelligent transport systems," Irish Interdisciplinary Journal of Science and Research, Vol. 6, Iss. 4, Pages 70-86, October-December 2022, doi: 10.46759/iijsr.2022.6409.

[24] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "Simplifying Handwritten Characters Recognition Using a Particle Swarm Optimization Approach", European Academic Research, Vol 1,pp. 535- 552, Issue(5), 5. 2013.

[25] Majda Ali Abed and Hamid Ali Abed Al-Asadi, "High Accuracy Arabic Handwritten Characters Recognition using (EBPANN) Architecture," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 6 Issue 2, 2015.

[26] Hamid Ali Abed Al-Asadi and Majda Ali Abed, "Object Recognition Using Artificial Fish Swarm Algorithm on Fourier Descriptors," American Journal of Engineering, Technology and Society; Volume 2, Issue 5: pp. 105-110, 2015.

[27] Vinod Varma Vegesna (2021). "Analysis of Data Confidentiality Methods in Cloud Computing for Attaining Enhanced Security in Cloud Storage," Middle East Journal of Applied Science & Technology, Vol. 4, Iss. 2, Pages 163-178, April-June 2021, Available at SSRN: https://ssrn.com/abstract=4418127

[28] Vinod Varma Vegesna (2021). "A Highly Efficient and Secure Procedure for Protecting Privacy in Cloud Data Storage Environments," International Journal of Management, Technology and Engineering, Volume XI, Issue VII, July 2021, Pages 277-287.

[29] Sparks, S., Embleton, S., Cunningham, R., Zou, C.: Automated vulnerability analysis: leveraging control flow for evolutionary input crafting. In: IEEE 23rd Annual Computer Security Applications Conference (2007).

[30] Turpe, S., Eichler, J.: Testing production systems safely: common precautions in penetration testing. In: IEEE Academy Industrial Conference (2009).

[31] Halfold, W., Choudhary, S., Orso, A.: Penetration testing with improved input vector identification. In: IEEE International Conference on Software Testing Verification and Validation (2009).

[32] International Organization for Standardization. IEC/ISO 27001:2013. http://www.iso.org/iso/home/store/catalogue_ics/cat alogue_detail_ics.htm?csnumber=54534.

[33] Vinod Varma Vegesna (2023). “Adopting a Conceptual Architecture to Mitigate an IoT Zero-Day Threat that Might Result in a Zero-Day Attack with Regard to Operational Costs and Communication Overheads,” International Journal of Current Engineering and Scientific Research, Volume-10, Issue-1, Pages 9-17.

[34] Vinod Varma Vegesna (2023). “Methodology for Mitigating the Security Issues and Challenges in the Internet of Things (IoT) Framework for Enhanced Security,” Asian Journal of Basic Science & Research, Vol. 5, No. 1, January-March 2023, Pages 85–102, doi: 10.38177/ajbsr.2023.5110.

[35] Vinod Varma Vegesna (2023). “Secure and Reliable Designs for Intrusion Detection Methods Developed Utilizing Artificial Intelligence Approaches,” International Journal of Current Engineering and Scientific Research, Volume-10, Issue-3, Pages 1-7.

[36] Hamzah F. Zmezm, Hareth Zmezm, Mustafa S.Khalefa, Hamid Ali Abed Al-Asadi, "A Novel Scan2Pass Architecture for Enhancing Security towards E-Commerce," Future Technologies Conference 2017, 29-30 November 2017 | Vancouver, BC, Canada, 2017.

[37] Hamid Ali Abed Al-Asadi, Majida Ali Al-Asadi, Nada Ali Noori , "Optimization Noise Figure of Fiber Raman Amplifier based on Bat Algorithm in Optical Communication network," International Journal of Engineering & Technology, Scopus, Vol 7, No 2, pp. 874-879, 2018.

[38] Vinod Varma Vegesna (2023). “A Critical Investigation and Analysis of Strategic Techniques Before Approving Cloud Computing Service Frameworks,” International Journal of Management, Technology and Engineering, Volume XIII, Issue IV, April 2023, Pages 132-144.

[39] Vinod Varma Vegesna (2023). “A Comprehensive Investigation of Privacy Concerns in the Context of Cloud Computing Using Self-Service Paradigms,” International Journal of Management, Technology and Engineering, Volume XIII, Issue VII, July 2023, Pages 173-187.

[40] McDermott, J.P.: Attack net penetration testing. In: Proceedings of the 2000 Workshop on New Security Paradigms. ACM Press, New York (2001).

[41] Liu, B., Shi, L., Cai, Z.: Software vulnerability discovery techniques: a survey. In: IEEE 4th International Conference on Multimedia Information Networking and Security (2012).

[42] Duan, B., Zhang, Y., Gu, D.: An easy to deploy penetration testing platform. In: IEEE 9th International Conference for young Computer Scientists (2008).

[43] Vinod Varma Vegesna (2022). “Using Distributed Ledger Based Blockchain Technological Advances to Address IoT Safety and Confidentiality Issues,” International Journal of Current Engineering and Scientific Research, Volume-9, Issue-3, Pages 89-98.

[44] Vinod Varma Vegesna (2021). “The Utilization of Information Systems for Supply Chain Management for Multicomponent Productivity Based on Cloud Computing,” International Journal of Management, Technology and Engineering, Volume XI, Issue IX, September 2021, Pages 98-113.

[45] Hamid Ali Abed Al-Asadi, et al., “Nature Inspired Algorithms multi-objective histogram equalization for Grey image enhancement”, Advances in Computer, Signals and Systems (2020) 4: 36-46 Clausius Scientific Press, Canada DOI: 10.23977/acss.2020.040106.

[46] Hamid Ali Abed Al-Asadi and et al., “ Critical Comparative Review of Nature-Inspired Optimization Algorithms (NIOAs), International Journal of Simulation: Systems, Science and Technology (IJSSST), 2020, 21(3), PP1-15

[47] Hamid Ali Abed Al-Asadi, (2022) “1st Edition: Privacy and Security Challenges in Cloud Computing A Holistic Approach" Intelligent Internet of Things for Smart Healthcare Systems, Scopus, Taylor @Francis, CRC Press. (Book Chapter: Enhanced Hybrid and Highly Secure Cryptosystem for Mitigating Security Issues in Cloud Environments), March 2022.

[48] Vinod Varma Vegesna (2021). “The Applicability of Various Cyber Security Services for the Prevention of Attacks on Smart Homes,” International Journal of Current Engineering and Scientific Research, Volume-8, Issue-12, Pages 14-21.

[49] Vinod Varma Vegesna (2020). “Secure and Privacy-Based Data Sharing Approaches in Cloud Computing for Healthcare Applications,” Mediterranean Journal of Basic and Applied Sciences, Volume 4, Issue 4, Pages 194-209, October-December 2020, doi: 10.46382/mjbas.2020.4409.

[50] Vinod Varma Vegesna (2019). “Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes”, Indo-Iranian Journal of Scientific

Research, Volume 3, Issue 1, Pages 69-84, January-March 2019, Available at SSRN: https://ssrn.com/abstract=4418119

[51] Geer, D., Harthorne, J.: Penetration testing: a duet. In: IEEE Proceedings of 18th Annual Computer Security Application Conference, ACSAC’02 (2002).

[52] LanFang, W., HaiZhou, K.: A research of behavior based penetration testing model of the network. In: IEEE International Conference on Industrial Control and Electronics Engineering (2012).

[53] Antunes, N., Vieira, M.: Benchmarking vulnerability detection tools for web services. In: IEEE International Conference on Web Services (2010).

[54] White Hat Statistics Report’ 2013. https://www.whitehatsec.com.